VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra Informatiky

Firewally pro malé a střední firmy
Firewalls for Small and Medium Companies

2010 **Jacek Rybicki**

Prohlašuji, že jsem tuto bakalářskou/diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 20.8.2010 _____

Jacek Rybicki

Děkuji panu Ing. Petru Grygárkovi, Ph.D. za předmětné připomínky a odbornou pomoc v průběhu psaní mé práce.

Abstrakt

Tato bakalářská práce se věnuje porovnání firewallů od společností Cisco, Check Point a Juniper Networks. Popisuje typy firewallů, jejich bezpečnostní mechanismy a porovnává rozdíly v konfiguracích bezpečnostních prvků jednotlivých firem. Praktická část se věnuje návrhu sítě pro malé a střední společnosti a penetračnímu testování firewallů. Rovněž popisuje bezpečnostní politiku pro důvěryhodnou a nedůvěryhodnou síť.

Abstract

This thesis compares firewalls from a Cisco, Check Point and Juniper Networks. It describes types of firewalls, their security mechanisms and compares differences in configurations of the security devices of individual companies. The practical part is devoted to design of network for a small and medium-sized companies and penetration testing of firewalls. It also describes the security policy for a trusted and untrusted network.

Klíčová slova

Firewall, zabezpečení sítě, bezpečnostní zóna, bezpečnostní politika, Check Point, Juniper Networks, Cisco, důvěryhodná zóna, nedůvěryhodná zóna, demilitarizovaná zóna, stavová inspekce, spojení, rozhraní, bezpečnostní mechanismy, inspekce aplikační vrstvy, překlad síťových adres, portfolio, sekvence průběhu paketu, IP adresa, malá a střední firma, penetrační testování

Key words

Firewall, network security, security zone, security policy, Check Point, Juniper Networks, Cisco, trusted zone, untrusted zone, demilitarized zone, stateful inspection, connection, interface, security mechanisms, application-layer inspection, network address translation, portfolio, packet flow sequence, IP address, small and medium business, penetration testing

Seznam použitých symbolů a zkratek

ACL (Access control list) – přistupové seznamy
ASA (Adaptive Security Appliance) – firewall společnosti Cisco
ASDM (Adaptive Security Device Manager) – grafické rozhraní pro management ASA
CLI (Command-line interface) – rozhraní příkazového řádku
DoS (Denial of Service) – typ útoku
DMZ (Demilitarized Zone) – demilitarizována zóna
DNS (Domain Name System) – překlad jmen na IP adresy
FTP (File Transfer Protocol) – protokol pro přenos dat
HTTP (Hypertext Transfer Protocol) – protokol pro výměnu hypertextových dokumentů
ICMP (Internet Control Message Protocol) – protokol IP sady
IOS (Internetwork Operating System) – operační systém společnosti Cisco
ISG (Integrated Security Gateways) - produktová řada společností Juniper Networks
IDP (Intrusion Detection and Protection) - produktová řada společností Juniper Networks
LAN (Local Area Network) – lokální síť
NAT (Network address translation) – překlad adres
NSM (NetScreen Security Manager) – nástroj pro vzdálenou správu
OS (Operating system) – operační systém
OSI (Open Systems Interconnection) – standardizace počítačových sítí a protokolů
PAT (Port Address Translation) – překlad adres s využitím portů
SMTP (Simple Mail Transfer Protocol) – protokol pro přenos zpráv elektronické pošty
SSG (Securure Services Gateway) – produktová řada společností Juniper Networks
SSH (Secure Shell) – zabezpečený komunikační protokol
TCP/IP (Transmission Control Protocol/Internet Protocol) – protokolová sada
UDP (User Datagram Protocol) – nestavový protokol IP sady
UTM (Unified Threat Management) – produktová řada společnosti Check Point
VPN (Virtual Private Network) – virtuální privátní síť
WAN (Wide Area Network) – rozlehlá síť

Obsah

1. Úvod

V dnešní době je mnoho výrobců na trhu, kteří produkují bezpečnostní prvky. Porovnávání a testování těchto zařízení je subjektivní, a to hlavně z důvodu veliké konkurence, kde platí pravidlo džungle, tzn. kdo má v dnešní době více finančních prostředků, má velikou výhodu oproti menším společnostem, které jsou na tom hůř. Chtěl jsem tím říct, že určitě existuje hodně jiných firewallů od menších společností, které jsou výkonnostně obdobné jako ty, které budeme testovat. Cenově budou úplně v jiné kategorii.

Budeme porovnávat firewally společnosti Cisco, Check Point a Juniper Networks, které jsou aktuálně největšími prodejci síťových prvků (Check Point pouze bezpečnostních) na světě pro podnikové sítě, ISP, data centra. Než, ale dojdeme k popisování technologií jednotlivých společnosti, tak si v úvodních kapitolách přiblížíme historii a mechanismy firewallů, které se do dnes některé používají.

V následujících kapitolách si popíšeme jednotlivé výrobce a jejich bezpečnostní mechanismy. Poté zvolíme vzájemně porovnatelné modely, které nakonfigurujeme podle navržené topologie sítě. Provedeme penetrační testování na firewallech s upravenými konfiguracemi a shrneme výsledky.

2. Historie firewallů

Firewall je zařízení, kterého funkce je omezit a zabezpečit přístup k síťovým zdrojům a také bránit před různými síťovými útoky. O firewallech se začalo mluvit až koncem 20. století, kdy v Internetu neexistovalo praktický žádné zabezpečení, a Internet zasáhl první virus, červ Morris. První firewally byly jednoduché přístupové seznamy (ACL), které zůstaly implementovaný do směrovačů. Toto řešení je pojmenováno jako filtr paketů.

3. Typy firewallů

V dnešní době existuje víc typů firewallů. Tím nejjednodušším je zmiňovaný filtr paketů, který dneska najdeme téměř v každém směrovači. Druhou generací jsou firewally, které přidaly další vrstvu zabezpečení. Jedná se o zařízení fungující na aplikační vrstvě, známe také jako aplikační proxy. Nejvíc úspěšnou a používanou technologii je stavová inspekce. Praktický jakýkoli hardwarový firewall je stavový firewall.

3.1. Filtr paketů

Tento typ firewallů funguje tak, že se dívá do hlaviček paketů a na základě získaných informací se rozhoduje, jestli paket propustí, nebo ne. Paketové filtry fungují na 3/4. vrstvě OSI modelu a většinou se rozhoduji jenom podle zdrojové, cílové IP adresy a cílového čísla portu. Výhody tohoto typu jsou výkon, kompatibilita a jednoduchost. Nevýhodou je slabé zabezpečení a absence podpory pokročilých (dynamických) protokolů.

3.2. Aplikační proxy

Je znám také jako proxy firewall. Je limitovaný počtem protokolů, které podporuje. Funguje tak, že každé spojení je ukončeno na firewallu a je navázáno nové. Přímé spojení skrze tento typ firewallu není možné. Většinou proxy servery podporují pouze TCP spojení. Funguje na 7. vrstvě OSI modelu.

Ukládá si do paměti spojení, které přicházejí, vytváří nové spojení do cílové stanice přímo z firewallu. Většinou tyto firewally nesměrují pakety. Jestli je potřeba, pakety upravují a následně posílají do destinace. Výhodou těchto aplikačních proxy je nejvyšší míra zabezpečení, protože si ukládají všechna spojení do paměti a také proto, že úplně rozumí protokolům a dohlíží na to, aby byly dodrženy všechny standardy. Nevýhodou je veliká náročnost na výkon. Tím, že porušuje model spojení klient/server, nebude zaručena funkčnost všech aplikací.

3.3. Stavová inspekce

Většina dnešních firewallů funguje stavově. Jedná se o sloučení obou předchozích typů. Tento je typ je schopný zaručit aplikační kontrolu bez porušení síťového modelu klient/server. Příchozí spojení jsou po úspěšném dokončení three-way handshake uloženy do stavové tabulky, která drží tyto spojení, dokud nezůstane spojení řádně ukončeno, nebo nevyprší časový limit spojení. Funguje na 3. – 7. vrstvě OSI modelu. Mezi největší výhody patří:

- Rychlost – stavový inspekce je integrovaná do jádra firewallu
- Podpora dynamických protokolů
- Bezpečnost – celý paket je prohlížený, když prochází bránou
- Transparence – paket se neupravuje (výchozí pravidlo)

4. Podporované mechanismy

Protože tato práce se bude zabývat bezpečnostními prvky pro ochranu malé a střední společnosti, budeme se zabývat i mechanismy, které firewall podporuje. Firewall není určen pouze pro kontrolu síťového provozu a zabezpečení firemních zdrojů. V mnoha případech plní roli internetové brány, na které se překládají IP adresy, ukončují VPN spojení a také se provádí směrování. Jedná se o universální zařízení, které nabízí hodně funkcí nespojených pouze se zabezpečením sítě. Protože si každý výrobce definuje jednotlivé mechanismy, přiblížíme si některé z nich při popisu společností Check Point, Juniper Networks a Cisco. Základní Principy těchto mechanismů ale fungují stejně.

4.1. NAT a PAT

- NAT (Network address translation) překlad síťových adres
- PAT (Port address translation) síťová maškaráda, dochází k mapování portů

Jedná se o překládání zdrojových nebo cílových IP adres na jiné IP adresy.

4.1.1. Překlad zdrojových adres (SNAT)

Tento způsob překladu použijeme, když chceme přeložit zdrojovou adresu. Používá se k přeložení privátní interní IP adresy na vnější veřejnou. Speciálním případem zdrojového překladu adres je PAT. Existuje přeložení jedna k jedné, anebo jedna k více IP adresám. Každý výrobce má svoje pojmenování zdrojového překladu adres. Budou probrány u jednotlivých výrobců.

4.1.2. Překlad cílových adres (DNAT)

Přeložení cílové adresy se používá, když chceme zveřejnit server, nebo službu nacházející se v privátní síti. V mnoha případech se překládají pouze některé porty, podle dostupných služeb.

V takovém případě mluvíme o přesměrování portu (port forwarding). Směrovač, nebo firewall přesměruje spojení, které má cílovou IP adresu stejnou jako jeho vnější rozhraní, do interní sítě.

4.1.3. Síťová maškaráda (PAT)

Je nejvíc používanou formou překladu, se kterou se můžeme setkat v počítačových sítích s privátním rozsahem IP adres. Je to přeložení vnitřní sítě na jednu IP adresu, která je ve většině případů také výchozí bránou do Internetu. Je to způsob, kdy všechny počítače v interní sítí sdílejí jednu (většinou veřejnou) IP adresu. Je to docíleno mapováním portů. Protože všechny počítače mají stejnou zdrojovou IP adresu, tak se k zdrojové IP adrese přidává číslo portu, které identifikuje spojení s počítačem. Tento způsob překladu také poskytuje zabezpečení pro interní síť, protože z pohledu Internetu a kohokoli zvenčí se tak jeví, jako jedná IP adresa.

4.2. Virtuální privátní sítě (VPN)

Jedná se o propojení počítačů, nebo sítí, které jsou odděleny nedůvěryhodnou sítí (Internetem). Řekněme, že se uživatel chce připojit do firemní lokální sítě někde z Internetu. Aby toto spojení bylo bezpečné, musí být uživatel ověřen, např. pomocí digitálních certifikátů a přenos dat musí být šifrován. Jestli je uživatel ověřen, vytvoří se tunel, který je šifrovaný. Takže přenos dat je bezpečný i když prochází Internetem, nebo jinou nedůvěryhodnou sítí.

5. Cisco

5.1. Představení společnosti

Firma Cisco Systems, Inc. byla založena v roce 1984 skupinou vědců ze Stanford University. Název společnosti vznikl jako zkratka z názvů města San Fran**cisco** a firemní logo znázorňuje Golden Gate brigde v témže městě. Je jednou z největších počítačových firem v dnešní době a také hraje velkou roli ve výrobě síťových prvků. Mimo jiné vyrábí přepínače, směrovače, firewally a také je zaměřená na VoIP technologie. V současné době zaměstnává kolem 66000 tisíc zaměstnanců. Hodnota společnosti se odhaduje na 135 miliard dolarů.

5.2. Portfolio firewallů

Firewall PIX byly představen na začátku roku 1994, rychle se stal jednou z vlajkových lodí v podnikové řadě firewallů. Produktové řada je rozdělená podle výkonností a použití (obr 1.). V dnešní době už se řady PIX firewallů nevyrábějí, v lednu roku 2008 společnost ukončila výrobu této řady. Důležitou poznámkou je fakt, že se firma zavázala pokračovat v podpoře těchto produktů až do 27. Srpna 2013.

Cisco PIX 501	Cisco PIX 506E	Cisco PIX 515E	Cisco PIX 525	Cisco PIX 525	Cisco PIX 535
Teleworker or SOHO (1–20 Users)	Small Branch Office (20–99 Users)	Medium-Sized Branch Office (100–999 Users)	Enterprise Branch Office (100–999 Users)	Enterprise Edge	Enterprise Headquarters Data Center
					

Obrázek 1

Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580
Small Office	Medium-Sized Branch Office	Enterprise	Enterprise Edge	Enterprise Edge or Headquarters	Data Center
					

Obrázek 2

V roce 2005 společnost představila řadu bezpečnostních prvků Adaptive Security Appliance (ASA), která v dnešní době nahradila firewally PIX. Firewally ASA (obr. 2.) vycházejí z PIXů řady 500, VPN koncentrátorů řady 3000 a IPS produktů řady 4200. O možnostech a funkcích této řady se budeme zabývat v dalších kapitolách. Tato řada rovněž rozděluje zařízení podle použití a také podle výkonností a propustností.

Společnost ještě produkuje jeden druh firewallu. Je to IOS Firewall. Jedná se o softwarové řešení pro směrovače s integrovanými služby řady 1800, 2800 a 3800 a také pro nejvyšší řadu směrovačů 7200 a 7600. IOS firewall poskytuje hodně stejných možnosti jako hardwarové řešení, která jsou integrovaná do operačního systému směrovače. Určitě si najde svoje použití, a to hlavně pro ochranu menších sítí kde není kladem vysoký důraz na výkon, ale na integrované řešení.

5.3. Popis bezpečnostních mechanismů

5.3.1. Směrovací a transparentní režim

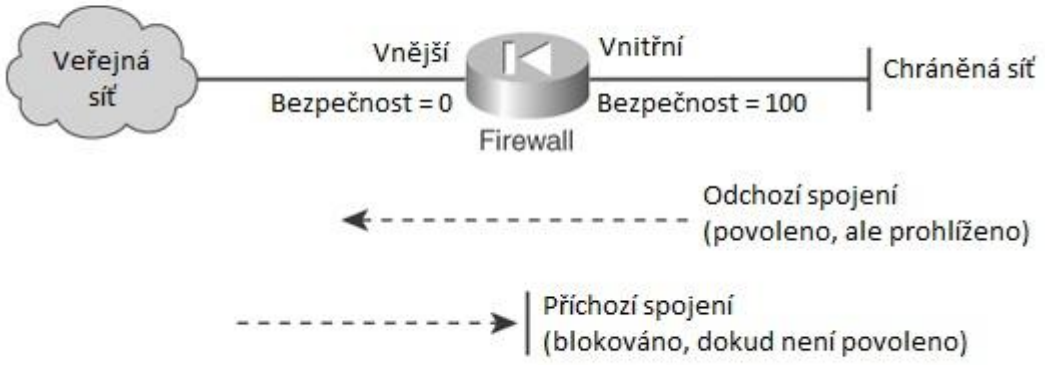
Firewall většinou operuje na třetí vrstvě, podporuje různé funkce jako je směrování, překlad adres, a další. Nastavují se IP adresy na rozhrání a tak funguje jako brána pro interní sítě. Tento režim se jmenuje směrovací a je to výchozí režim.

Firewall může také vystupovat v transparentním režimu. V tomto režimu zařízení vystupuje na druhé vrstvě, ale filtrace není omezena pouze na tuto vrstvu. Jenom dvě rozhrání jsou povolená, vnitřní a vnější. Nenastavují se IP adresy na tyto rozhrání, firewall nerozděluje síť a tak pro běžnou stanici je neviditelný. Nepodporuje žádné možnosti pracující na třetí vrstvě, jako je dynamické směrování, překlad adres, atd. Jenom pro správu se může nastavit adresa třetí vrstvy. Abychom mohli směrovat provoz pro správu zařízení, můžeme vytvořit statické cesty.

5.3.2. Sekvenční průběh paketu

Firewall má dvě, nebo více síťových rozhraní, mezi kterými kontroluje provoz. Nejjednodušší verze má jedno vnější a druhy vnitřní rozhraní. Každé rozhraní má přiřazenou hodnotu, která určuje míru bezpečnosti. Hodnota se pohybuje mezi 0 a 100. Vnější (outside) rozhraní není lokální a má vždycky hodnotu 0. Provoz, který přichází z tohoto směru, není bezpečný a musí být zkontrolován. Vnitřní (inside) rozhraní má hodnotu 100, do něho je připojená naše interní síť a proto provoz je považován za bezpečný. Obrázek 3. představuje firewall se dvěma rozhraními. Cisco představuje svoje firewally většinou symbolem diody[1], která má vlastnost, že propouští proud jenom jedním směrem. Proto síťový provoz, který jde ve směru šipky je povolen a provoz jdoucí proti šipce je zakázán. Výchozí chování firewallu si můžeme shrnout:

- Odchozí spojení, přicházející z rozhraní z vyšší bezpečnosti a vycházející rozhraním s menší bezpečnosti jsou povoleny
- Příchozí spojení, přicházející z méně zabezpečeného rozhraní a vycházející více zabezpečeným rozhráním jsou blokovány



Obrázek 3

Výchozí bezpečnostní pravidla můžeme vždy změnit a nastavit, aby některá odchozí spojení byla blokována a příchozí povolena, taky můžeme nastavit obě rozhraní na stejnou úroveň bezpečnosti a tím docílíme, že provoz mezi nimi bude povolen. Každý provoz je kontrolován stavovou inspekcí, běžně nazývanou kontrolou protokolů aplikační vrstvy.

Cisco firewall kontroluje síťový provoz řadou funkcí, které jdou za sebou v určitém pořadí. Představme si situaci, že paket přichází na vnější rozhraní a chce pokračovat do vnitřní sítě. Firewall bude provádět následující kroky:

1. Vstupní kontrola
2. Xlate tabulka (pouze odchozí spojení)
3. Stavová tabulka spojení

4. ACL (přístupové seznamy)
5. Xlate tabulka (pouze příchozí spojení)
6. Kontrola oprávnění
7. Inspekční nástroj

Vstupní kontrola – v první fázi se kontroluje integrita paketu. Jedna z nejdůležitějších věcí, které můžou být prověřené, je integrita zdrojové adresy paketu. Toto prověření provádí mechanismus RPF (Reverse Path Forwarding). Funguje tak, že se podívá do směrovací tabulky a porovná rozhraní, ze kterého přišel s rozhraním, na které by směroval tento paket. Jestli se tyto rozhrání shodují, posílá paket dál, jestli ne, zahazuje paket s označením podvržený (spoofing). Bohužel tento mechanismus ne dokonce funguje pro vnější rozhraní, které většinou bývá výchozí bránou a vede do Internetu. Firewall nemůže rozpoznat podvržení zdrojové adresy, jestli přijde skrze toto rozhrání, protože nezná informace o všech sítích, které se za ním skrývají.

Vyhledávaní v tabulkách – následující fází je vyhledávání v tabulkách xlate (překlad adres), stavové a v přístupových seznamech. Překládací tabulka obsahuje záznamy o všech spojeních, které se překládají (provádí se na nich NAT). Pořadí, kdy se vyhledává v této tabulce, se liší, podle toho jestli je to odchozí spojení (vyvolané ve vnitřní síti), nebo příchozí (inicializované ve vnější síti). Pro odchozí se porovnává po vstupní kontrole, protože přeložena adresa se používá při vytvoření záznamu spojení v přístupových seznamech. Při příchozím spojení je to opačně. Překládá se později, nejdřív se koukne do přístupových seznamů a porovnává nepřeložené adresy.

Stavová tabulka obsahuje záznamy o stavech spojení. Jestli bude spojení povoleno (přístupový seznam povolí provoz) tak se automatický vytváří záznam. Firewall si pamatuje toto spojení a upravuje si jeho stavy. Záznam se smaže, když je spojení neaktivní a vyprší časový limit spojení. Běžně se tomu kroku říká stavová inspekce, protože se firewall vždy prohlíží tuto tabulku a když zjistí, že spojení už bylo úspěšně navázáno a existuje o něm záznam, tak pakety propouští. Prakticky všechny dnešní firewally používají tento mechanismus.

ACL - Než může být spojení úspěšně navázáno, musí být provoz povolen přístupovými seznamy. Tento krok porovnává zdrojovou, cílovou adresu a port cílové služby s ACL (access list).

Kontrola oprávnění – když je nastavena autentizace uživatele při inicializaci spojení, prochází spojení kontrolou oprávnění. Jestli je autentizace úspěšně zakončena, firewall si uloží uživatelské údaje do paměti, a při dalším spojení už nebude vyžadovat autentizaci. Cisco firewally podporují ověřovaní vůči RADIUS a TACACS+ serverům.

Inspekční nástroj – posledním krokem je kontrola protokolů aplikační vrstvy. Jedná se o kontrolu spojení podle stanovených principů jednotlivých protokolů. Protokoly můžeme dělit na nespojové a spojové. Příkladem nespojových protokolů je například UDP, nebo ICMP, které nemají striktní doporučení pro vedení spojení mezi hostiteli. Naopak spojové protokoly, do kterých patří i TCP, mají jednoznačně striktní podmínky, co se týká navazování spojení a vyměňování paketů mezi zdrojem a cílem. Inspekce provozu může provádět kontrolu také dalších protokolů.

5.3.3. Překlad adres

Když dvě zařízení komunikují mezi sebou, provádí se překlad adres, dokonce i když IP adresy zůstanou stejné, tento proces se provede. Jedinou výjimkou je když se komunikuje mezi rozhraními,

které mají nastavené stejné číslo bezpečnosti. V tom případě se překlad může provádět, ale není vyžadován[2].
Pro připomenutí provoz se identifikuje podle toho, za kterým rozhraním se inicializuje. Předveden na obr. 3.

Základní typy překladu adres:

- Statický NAT
- NAT pomocí politiky
- Dynamický NAT
- PAT

Statický NAT
Může být použitý, když vnitřní, nebo vnější hostitel potřebuje, aby při každém spojení byla jeho adresa přeložena na stejnou adresu. Tento typ podporuje jak příchozí, tak odchozí spojení. Každé statický překlad, který je nakonfigurován, vytváří nový záznam v xlate tabulce.

NAT pomocí politiky
Tento překlad závisí od toho, jak je nastavená politika. Vytvoříme překládací politiku pomocí přístupových seznamů. Poté tímto seznamem specifikujeme, který provoz bude přeložen a na jakou adresu se bude mapovat. Tímto způsobem můžeme vytvořit pravidla, která nám vytvoří politiku, podle které se zdrojová adresa bude mapovat. Jedná se stále o mapování jedné adresy ku jedné adrese.

Dynamický NAT a PAT
Tento typ překladu se používá, když chceme, aby interní síť sdílela rozsah IP adres (Dynamický NAT), nebo abychom ji skryli za jedinou adresou, většinou je to adresa vnějšího rozhrání (PAT).
V případě dynamického překladu, interní hostitelé si propůjčují adresy z rozsahu, který je přidělený pro překlad. Poté co spojení exspiruje, propůjčena adresa se vrací zpět a může si jí propůjčit jiný hostitel. Při špatném rozvržení rozsahu, se může stát, že hostitelé nebudou mít k dispozici žádnou volnou adresu a spojení se zamítne.

6. Juniper Networks

6.1. Představení společnosti

Juniper Inc. je mezinárodní společnost, která byla založena v roce 1996. Hlavní sídlo se nachází v městě Sunnyvale, California ve spojených statech. Zabývá se vývojem a prodejem výkonných IP síťových zařízení a služeb. Mezi hlavní produkty patří směrovače v řadách T-série, M-série, E-serie, MX-série a J-série, přepínače EX-série a firewally.

6.2. Portfolio firewallů

Společnost poskytuje čtyři hlavní série firewallů. Tři, které používají ScreenOS operační systém, je to SSG, ISG a NetScreen série. Čtvrtá SRX série používá operační systém JUNOS, který se nachází také v přepínačích a směrovačích. Kromě operačního systému se SRX série rozlišuje tím, že tyto zařízení integrují firewall (**S**), směrovač (**R**) a přepínač (**X**). SSG série je cílená hlavně pro malé a střední

společnosti, budeme se o ni nejvíc zajímat. Firewally ISG série jsou schopny větší funkcionality a výkonu zejména v IDP a ve virtuálních systémech. NetScreen série je předurčená pro data centra a velké podnikové sítě.

Přehled jednotlivých sérií a produktů najdeme na internetových stránkách výrobce[3].

6.3. Popis bezpečnostních mechanismů

V této kapitole se budeme zabývat operačním systémem ScreenOS verze 6.1.0 [4], jeho architekturou a jednotlivými bezpečnostními mechanismy 3/4. a 7. vrstvy.

6.3.1. Bezpečnostní zóny

Stavebním kamenem pro Juniper firewally jsou bezpečnostní zóny. Bezpečnostní zóna je kolekcí jednoho, nebo více síťových segmentů, které vyžadují kontrolu příchozího a odchozího spojení pomocí bezpečnostní politiky. Je to logická jednotka svázaná s jedním, nebo mnoha síťovými rozhraními. Počet zón není nijak omezený (v rámci licence). Můžeme použít předdefinované zóny Trust, Untrust a DMZ, nebo si můžeme vytvořit nově nadefinované zóny. Případně je dovoleno použít obojí. Síťová rozhraní, která jsou přiřazeny k jednotlivým zónám, můžou být fyzické, nebo logické (sub rozhraní svázané s virtuální sítí, síťový tunel).

Existuje ještě jedna univerzální zóna. Globální zóna, je zónou, ke které není přiřazený žádný síťový segment nebo rozhraní. Bezpečnostní pravidla pro tuto zónu se vztahují k jakémukoli provozu procházejícímu firewallem.

6.3.2. Bezpečnostní politiky

Při vytváření politik povolujeme, nebo zakazujeme provoz mezi jednotlivými zónami. Výchozí pravidlo na firewallech této společnosti je zákaz veškerého provozu. Pokaždé, když se paket pokusí projít z jedné zóny do druhé, firewall prochází politiku a zjišťuje, jestli je tento provoz povolený. Takže pro každý provoz je nutné vytvořit pravidlo.

6.3.3. Virtuální systémy

Juniper u některých modelů podporuje možnost virtuálních systémů (vsys). Virtuální systém je samostatnou entitou, která má svoje bezpečnostní pravidla, směrovací tabulku a další systémové nastavení. Systému můžou mezi sebou sdílet jednotlivé zóny, rozhraní a virtuální směrovače. Zařízení pro malé a střední společnosti tuto funkci nepodporují, tak se o ni dál zabývat nebudeme.

6.3.4. Sekvenční průběh paketu bezpečnostními zónami

Pomocí pár bodů si shrneme, jak paket prochází firewallem.

1. Modul rozhraní zjišťuje zdrojové rozhraní a přiřazuje k němu zónu. Používá následující kritéria pro zvolení zdrojové zóny:
    - Pokud paket není zapouzdřený, bezpečnostní zdrojovou zónou je zóna, která svázána s příchozím rozhráním, nebo sub rozhraním
    - Pokud paket je zapouzdřený a tunelové rozhraní je svázané s VPN tunelem, tak bezpečnostní zdrojovou zónou je zóna svázána s tunelovým rozhraním
    - Pokud paket je zapouzdřený a tunelové rozhraní je svázané tunelovou zónou, tak bezpečnostní zdrojová zóna koresponduje se nosnou zónou (bezpečnostní zóna, která zastřešuje tunelovou zónu) pro tuto tunelovou zónu

2. Pokud jsou zapnuté SCREEN možnosti pro zdrojovou zónu, bezpečnostní zařízení aktivuje SCREEN modul v tomto okamžiku. Jestli SCREEN mechanismus detekuje anomální chování paketů, tak postupuje následovně:
    - zahodí paket a vytvoří záznam v logu
    - paket se nezahazuje, ale vytvoří se záznam o události a postupuje se k dalšímu kroku
3. Vyhledávání se v tabulce relací pro tento paket.
    - Pokud paket nepatří k žádné relaci, postupujeme kroky 4-8
    - Pokud paket patří k vytvořené relaci, tak se spouští rychlý procesní funkce, která obchází kroky 4-8
4. Pokud je použité mapované IP (MIP), nebo virtuální IP (VIP), tak modul pro mapování adres rozhodne o MIP a VIP adresách
5. Vyhledání cesty, nejdřív firewall zjišťuje, jestli je aktivována funkce PBR (Policy based rating), směrování založené na politiky. Protože tuto funkci je úzce spjata s virtuálními systémy, budeme předpokládat, že je vypnutá. Druhá fáze je vyhledaní pomocí směrovací tabulky rozhrání, které vede k cílové IP adrese, a zjistíme, která zóna je spjata s tímto rozhraním. Kroky ke zjištění cílové zóny jsou stejné jako u bodu 1. Rozdíl je v případě, když se zdrojová a cílová zóna shodují. V tom případě rozhoduje, jestli je zakázaný provoz v rámci jedné zóny. Pokud ano, firewall obchází kroky 6 a 7 a vytváří relaci (krok 8). V opačném případě paket je zahozen.
6. Vyhledávání v politice pravidla pro adresy a zdrojovou a cílovou zónu. Když pravidlo není nalezeno, paket se zahazuje. Když existuje, záleží od akce specifikované v pravidle.
7. Pokud je specifikovaný překlad adres, provádí se nejdřív překlad cílové adresy (NAT-dst) a potom překlad zdrojové adresy (NAT-src)
8. Modul relací vytváří nový záznam v tabulce relací, který obsahuje výsledky kroků 1-7. Tyto informace jsou posléze využity při správě následujících paketů stejné relace.
9. Firewall pokračuje v operacích specifikovaných v sezení.

6.3.5. Překlad adres

Bezpečnostní zařízení společnosti Juniper podporují standardní typy překladu adres. Popíšeme si jednotlivé typy IP adres, které jsou používány při NAT.

- DIP (Dynamic IP)
- MIP (Mapped IP)
- VIP (Virtual IP)

DIP rozsah se používá při zdrojovém překladu adres. Tento objekt obsahuje rozsah IP adres, na které se bude překládat originální IP. Když při zdrojovém překladu není tento rozsah uveden, automatický se použije PAT na odchozím rozhraní.

MIP se používá při cílovém překladu adres. Jedná se o vytvoření IP adresy, která je ze stejného síťového rozsahu, jako je rozhraní, na kterém MIP vytváříme. Tuto možnost můžeme použít, když máme privátní rozsah v zóně a chceme, aby nějaká služba byla dosažitelná z Internetu.

VIP se používá při cílovém překladu adres. Funguje v podstatě jako přesměrování portů. Vytváří se pouze v globální zóně, tzn. je v podstatě jedno, z jaké síťového rozsahu použijeme VIP. Když vytvoříme VIP, je to jako bychom vytvořili virtuální server, který směruje jednotlivé porty dál na

fyzické servery s jinými IP adresami. Například Pro HTTP spojení bude přesměrované na jeden server, pro FTP na jiný server, atd.

6.3.6. Mechanismus SCREEN

Pro sledování všech spojení, Juniper Networks bezpečnostní zařízení používají dynamické filtrovaní paketů, obecně známo jako hluboká inspekce. Při použití této metody firewall zaznamenává mnoho atributů v IP paketu a TCP hlavičce. Spravuje taky stav každé TCP sezení a UDP spojení.

SCREEN možnosti se aktivuji v rámci každé bezpečnostní zóny. Zabezpečují ji pomocí inspekce a posléze povolením, nebo zakázáním spojení procházejícím jakýmkoli rozhraním v rámci zóny.

Každá bezpečnostní politika může poskytovat obsahové filtrování pro provoz, který prochází SCREEN filtry.

Juniper Networks poskytuje mnoho obranných mechanismů proti základním útokům[4].

Síťová obrana ScreenOS funguje na dvou úrovních: bezpečnostní zóny a politiky. Celkově to můžeme shrnout, že útoky v rámci 3. a 4. vrstvy, se nastavují v rámci bezpečnostní zóny a inspekce 7. vrstvy v rámci bezpečnostních politik.

7. Check Point

7.1. Představení společnosti

Společnost založena v roce 1993 v Izraeli, kde se do teď nachází jejich hlavní sídlo. Patentovala stavovou inspekci, jako první ji použila ve Firewall-1, který také podporoval filtrování provozu na aplikační vrstvě. V dnešní době vyrábí softwarové a hardwarové bezpečností produkty a také produkty pro jejich správu.

V roce 1999 vznikla společnost SofaWare, která začala úzce spolupracovat s Check Pointem a vyvíjet softwarové řešení pro malé společnosti.

7.2. Portfolio firewallů

Check Point rozděluje svoje produkty do jednotlivých kategorií, které obsahují bezpečnostní prvky podle funkčního použití. Popíšeme si produkty v jednotlivých řadách[5]:

- Security gateways (bezpečnostní brány)
- Endpoint Security (koncové zabezpečení)
- Security Management (správa bezpečnostních prvků)

7.2.1. Bezpečnostní brány (Security gateways)

Tyto produkty kvůli svoji komplexnosti a flexibilitě, můžou vyhovět mnoha společnostem. Jedná se o dedikované hardwarové zařízení s před instalovaným softwarovým balíčkem (Security Appliances), nebo jako samostatné softwarové části (Security Software Blades).

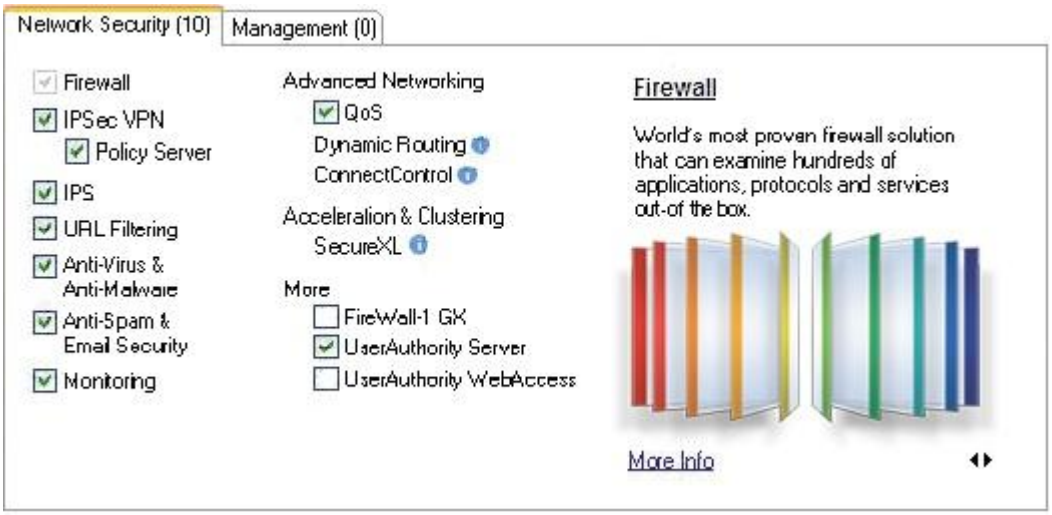
7.2.2. Koncové zabezpečení (Endpoint Security)

Jedná se o softwarové bezpečnostní řešení pro koncové zařízení. Jednotlivé produkty se zaměřují na šifrování disků a dat, personální firewall, antivirus, podporu VPN a další. Poskytují rovněž centralizovanou správu všech funkcí.

7.2.3. Správa bezpečnostních prvků (Security management)

Check point řešení pro správu prvků integruje konfiguraci, logování a reportování bezpečnostních politik. Jedná se buďto o dedikované hardwarové řešení (Smart-1 Appliances), nebo o softwarové balíčky, které obsahují jednotlivé nástroje pro správu.

V roce 2009 společnost Check Point předvedla novou architekturou tzv. architektura softwarových nožů (Software blades). Výhodou této architektury je možnost rozšíření bezpečnostní zařízení o nové funkce bez nutnosti přidávání nového hardwaru. Softwarový blade je samostatnou modulární jednotkou, která může být rychle aktivována jediným kliknutím v management konsoli (obr.4). Podle potřeb můžeme tyto softwarové nože jakkoliv upravovat[6].



Obrázek 4

Softwarové nože můžou být nasazeny v následujících produktech UTM-1™, Power-1™, Nokia IP zařízení a na jiných kompatibilních serverech. Není nutné investovat do dedikovaných zařízení, postačí zakoupit server, který je kompatibilní s operačním systémem SecurePlatform. Tento operační systém je možné si stáhnout na Internetových stránkách výrobce, nutná registrace. Je možné si jej vyzkoušet zdarma po určitou dobu. Tento systém už v sobě obsahuje jak softwarové nože pro síťové zabezpečení tak management centrum pro správu. Aktuální nejnovější verze platformy je R71.

7.3. Popis bezpečnostních mechanismů

Bezpečnostní mechanismy jsou dostupné podle jednotlivých softwarových balíčků a zakoupených licencí. Protože se orientujeme na malé a střední společnosti, je výběr omezený. Praktickou část

budeme testovat na dedikovaném zařízení **UTM-1™ Edge**, které obsahuje operační systém vyroben společnosti SofaWare, proto se budeme zajímat o mechanismy, které se týkají tohoto zařízení[8].

7.3.1. Bezpečnostní politika

Bezpečnostní politiku tvoří jednotlivá bezpečnostní pravidla. Pomocí bezpečnostních pravidel definujeme bezpečnostní požadavky počítačové sítě. Pravidla zahrnují zdrojovou a cílovou adresu, službu a akci, která platí pro každé spojení definující toto pravidlo. Báze pravidel je implementací bezpečnostní politiky. Pro uplatnění a kontrolu provozu mezi sítěmi Check Point používá patentovaný nástroj INSPECT. Tento nástroj prověřuje všechny komunikační vrstvy, extrahuje pouze relevantní data, což umožňuje vysoce efektivní provoz.

7.3.2. Výchozí bezpečnostní politika

Zařízení UTM-1 má přednastavené výchozí bezpečnostní pravidla:

- Přístup z WAN (vnější síť) je zakázaný do všech interních síti(DMZ, VLAN, WLAN).
- Přístup je povolen z vnitřní sítě do WAN, podle bezpečnostní úrovně firewallu.
- Z LAN je povolen přístup do jiných interních sítí.
- HTTPS spojení na UTM-1 Portal je povoleno z interních sítí.
- HTTP spojení na UTM-1 Portal je povoleno z interních sítí, kromě WLAN.

Většina těchto pravidel není ovlivněna bezpečnostní úrovní firewallu. Můžeme kdykoli změnit vytvořením bezpečnostního pravidla.

7.3.3. Bezpečnostní úrovně firewallu

Při konfigurace UTM-1 musíme nastavit úroveň firewallu. Můžeme použít následující úrovně:

Nízká (LOW)
Všechna spojení odchozí i příchozí spojení jsou povolena, kromě spojení na IP adresu vnějšího rozhraní firewallu, které je zakázáno, s výjimkou ICMP echo paketů (ping).

Střední (MEDIUM)
Všechna příchozí spojení (směrem do LAN) jsou zakázána. Všechna odchozí (směrem do WAN) jsou povolena, kromě sdílení souborů (NetBios přes TCP/IP)

Vysoká (HIGH)
Všechna příchozí spojení jsou zakázána. Omezená jsou všechna odchozí spojení s výjimkou web provozu (HTTP, HTTPS), elektronické pošty (IMAP, POP3, SMTP), FTP, TELNET, DNS, forum, IPSEC IKE a VPN provozu.

Blokovat vše (Block All)
Veškerý provoz je blokován, kromě spojení jejichž iniciátorem je firewallem.

7.3.4. Překlad adres (NAT)

Podporovaná pravidla pro překlad adres jsou následující:

Statický NAT (One-to-One)
Překlad rozsahu zdrojových privátních IP adres na stejně velký rozsah veřejných IP adres.

Hide (Skrytý) NAT (One-to-Many)
Překlad rozsahu zdrojových adres na jednu adresu. Stejná mechanismus jako PAT.

Few-to-Many NAT
Překlad menšího rozsahu IP adres na větší rozsah. Zbytek nepřeložených IP adres ve větším rozsahu zůstává.

Many-to-Few NAT
Překlad většího rozsahu IP adres na menší rozsah. Všechny IP adresy z většího rozsahu se budou postupně překládat na IP adresy z menšího, dokud nedojde na poslední adresu v menším rozsahu. Na tu poslední se potom aplikuje Hide NAT, takže zbytek adres z většího rozsahu se bude překládat na jednu, poslední adresu.

Service-based NAT
Překlad originální služby, na kterou se spojení navazuje na jinou službu. Obdoba přesměrovaní portů.

7.3.5. SmartDefense (Chytrá obrana)
Tento mechanismus poskytuje obranu proti útokům na 3/4. a 7. vrstvě. Obsahuje nástroje, které chrání síť následujícími způsoby:

- Ověřuje shody se standardy
- Ověřuje očekávané použití protokolů (Protocol Anomaly Detection)
- Omezuje schopnost aplikací přenášet nebezpečná data
- Kontroluje operace na aplikační vrstvě

Útoky jsou rozdělené do jednotlivých kategorií. Při aktivaci této funkce pomocí grafického rozhraní můžeme použít průvodce, který nám dovolí si vybrat z jednotlivých úrovní nastavení. Máme možnost i manuální nastavení, ale společnost Check Point nám nedává příliš prostoru pro upravení parametrů jednotlivých útoků.

8. Volba srovnatelných firewallů
Pro srovnání jsme zvolili modely, které jsou porovnatelné jak funkcemi a technickými parametry, tak dostupnosti a zaměřením na malé a střední společnosti. Společnosti Check Point, Juniper Networks a Cisco jsou v dnešní době vedoucími společnostmi, co se týká síťových produktů na trhu. Jejich produkty (u Juniper Networks a Cisco, nejenom bezpečnostní prvky) jsou vlajkové lodě mezi síťovými prvky, které jsou především zaměřené na velké podnikové sítě, data centra a poskytovatele Internetového připojení (ISP). A to je taky jedna z příčin vyšší ceny i u těch nejméně výkonných modelů.

Pro porovnání jsme zvolili:

8.1. Cisco
ASA 5505 – model pro malé společnosti a firemní pobočky. Poskytuje 8 síťových rozhraní, z toho 2 můžou být využity pro napájení po sítí. Rychlost rozhraní 10/100 Mbps. V základní (Base) licenci můžeme použít až tři virtuální sítě (vlan), do kterých můžeme libovolně přiřadit fyzické porty. Pro

jednotlivě vlany vytvoříme virtuální rozhraní, na kterých nastavíme úroveň zabezpečení. Toto řešení poskytuje velkou flexibilitu návrhu sítě. Výpis licence použitého zařízení se nachází v příloze.

8.1.1. Možnosti konfigurace

Model ASA 5505 poskytuje více možnosti, jak jej spravovat. V této kapitole si je přiblížíme. Možnosti jsou následující:

- CLI (Command Line Interface) – příkazový řádek, přístup pomocí konz1olového připojení, SSH (Secured Shell) a Telnet
- Adaptive Security Device Manager (ASDM) – grafické rozhraní přístupné přes webový prohlížeč
- Cisco Security Manager (CSM)

Uživatelské rozhrání poskytuje více režimů, které jsou stupňované podle možností konfigurace a použitelných příkazů.

Uživatelský EXEC režim – při výchozím nastavení se uživatel po připojení dostane do tohoto režimu, velice omezený počet příkazů.

```
Firewall>
```

Privilegovaný EXEC režim – uživatel se může dostat pomocí příkazu **enable** v uživatelském režimu, po úspěšném zadání hesla má plné práva pro spouštění všech příkazů. Syntaxe pro vstoupení je následující:

```
Firewall> enable
password: password
Firewall#
```

Konfigurační režim – z privilegovaného režimu je možné se dostat do konfiguračního, ve kterém nám zařízení poskytuje možnost konfigurovat síťová rozhrání a jakékoli další vlastnosti. Pro vstup použijeme syntaxi:

```
Firewall# configure terminal
Firewall(config)#
```

Výchozí uživatelské jméno a heslo

Při výchozím nastavení, je nastavené následující uživatelské jméno a heslo:

login: <prazdný>
heslo: cisco

8.2. Juniper Networks

SSG5 – model pro malé společnosti a firemní pobočky. Nabízí sedm fyzických rozhraní s rychlostí 10/100 Mbps. Při využití bezpečnostních zón, kterých můžeme vytvořit osm, je taky využití tohoto

zařízení velice flexibilní. Pro naše potřeby jsme měli model s rozšířenou licencí, ale to nijak neovlivnilo výkon při testování. Výpis licence se rovněž nachází v příloze.

8.2.1. Možnosti konfigurace

Firewall je možné konfigurovat ve dvou uživatelských rozhraních:

- WebUI – grafické uživatelské rozhrání, přístupné pomocí internetového prohlížeče
- CLI – rozhraní textové, příkazový řádek
- NSM – administrace pomocí NetScreen Security Manageru

WebUI - přístupné pomocí internetového prohlížeče, použít můžeme jak nezabezpečené spojení HTTP (port tcp/80), tak i zabezpečené HTTPS(port tcp/443)

CLI – při konfiguraci pomocí příkazové řádky pomocí konsole můžeme použít jakoukoli aplikace, která dovede emulovat terminál VT100. Pro vzdálený přístup se můžeme připojit nešifrovanou spojením pomocí aplikace telnet, nebo využít zabezpečený způsob pomocí klienta SSH.

NSM – administrace pomocí aplikačního klienta NSM, který se připojuje na management server. NSM server může být napojen na více firewallů najednou. Je to možnost sjednocení správy více bezpečnostních prvků do jednoho bodu. Využívané ve velkých podnikových sítích a data centrech.

Výchozí uživatelské jméno a heslo

Při výchozím nastavení, je nastavené následující uživatelské jméno a heslo:

login: netscreen
heslo: netscreen

Po úspěšném přihlášení pomocí CLI, se zobrazí:
device_name->

8.3. Check Point

UTM-1 Edge W – dedikované zařízení s operačním systémem od SofaWare, ale s technologiemi společnosti Check Point. Pro porovnání z ostatními firewally, jsme vybrali právě porovnatelné zařízení pro malé společnosti a firemní pobočky. Tento model poskytuje šest rozhraní, o rychlostí 10/100 Mbps. V případě tohoto modelu, se jedná o verzi s možností bezdrátového připojení pro max. 16 uživatelů. Čtyři rozhraní jsou v přepínači, který je přiřazen do LAN sítě. Jednoho WAN rozhraní a jednoho DMZ\WAN2 rozhraní. To řešení není až tak flexibilní jako u ostatních modelů, ale porty v přepínači můžeme přiřadit k dalším sítím. Rozhraní DMZ/WAN2 může využito jako rozhraní DMZ, nebo jako kmenové (trunk) rozhraní pro virtuální sítě. Informace o zařízení se nacházejí v příloze.

8.3.1. Možnosti konfigurace

Zařízení můžeme konfigurovat třemi způsoby:

- Příkazový řádek (CLI)
- Grafické rozhraní (UTM-1 Portal)
- Centrální řízení (SmartCenter)

Příkazový řádek (CLI)

Konfigurace zařízení pomocí CLI, vyžaduje znalost jednotlivých příkazů[7]. Můžete se připojit buďto pomocí konsole (lokálně), nebo pomocí SSH klienta. Výchozí nastavení rychlostí sériového portu je 57600 bps. Pro připojení k sériové konzoli použijte kabel RS-232. Vzdálené připojení pomocí SSH vyžaduje protokol SSHv2, SSHv1 není podporovaný z důvodu bezpečnostního rizika. Služba SSH naslouchá na portu tcp/22.

Grafické rozhraní

Abychom se mohli připojit k UTM-1 grafickému portálu, použijeme protokol HTTP(tcp/80), nebo HTTPS(tcp/443). Použijeme internetový prohlížeč a jako URL zvolíme IP adresu vnitřního, nebo vnějšího rozhraní. Připojení z Internetu (vnější rozhraní) vyžaduje zabezpečené spojení pomocí HTTPS protokolu.

Centrální řízení

Check Point poskytuje softwarový produkt pro centrální řízení jejich zařízení. Jedná se o SmartCenter, které poskytuje veškeré potřebné nástroje pro editaci bezpečnostních politik, konfigurace zařízení, monitorování, správa log záznamů a další. UTM-1 Edge můžeme taky připojit k SmartCenter serveru. Doporučuje se používat dedikovaný server, ale je taky možnost aktivovat SmartCentrum přímo na dedikovaném zařízení. Jedná se o softwarový blade pro správu.

9. Praktická část

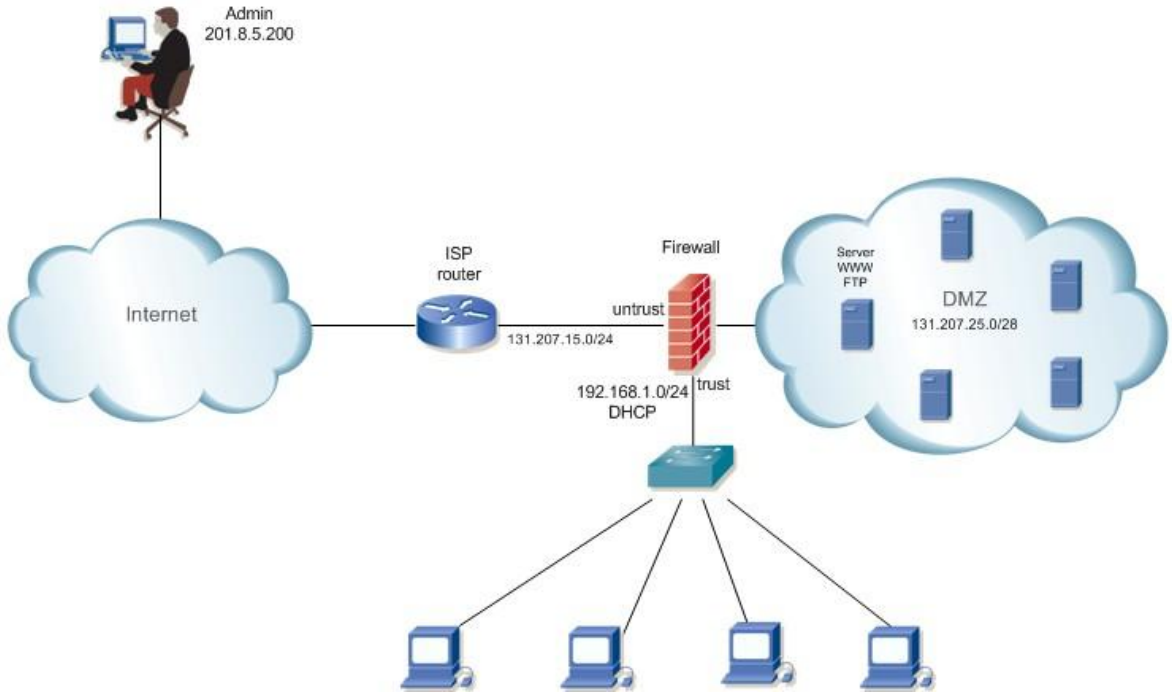
Tuto část rozdělíme do více oddílů:

- Navržení lokální sítě a IP rozsahů
- Bezpečnostní pravidla pro vnitřní a vnější síť
- Konfigurace firewallu
- Testovaní bezpečnostních mechanismů

Pro omezení bezpečnostních děr v naší síti bychom se měli pozastavit nad každým z těchto bodů, protože nesprávné rozhodnutí může vést k útoku na firewall nebo síťové zařízení dostupné z internetu. Protože se jedná o firewalle pro malé a střední společnosti, jakýkoli útok vede minimálně k zatížení bezpečnostního zařízení, což sebou nese zpomalení síťového spojení, nebo dokonce nefunkčnost celé lokální sítě.

9.1. Navržení lokální sítě a IP rozsahů

Jak už bylo zmíněno firewall v malých a středních společnostech plní většinou funkci internetové brány, která odděluje vnitřní síť od Internetu. Jedná se hlavně o úsporu finančních prostředků, ale také o výhodu pro administrátora, protože se veškerá správa zužuje na jeden síťový prvek, pomocí kterého se správce může případně připojit na další síťové zařízení.



Obrázek 1

Mějme návrh pro malou, nebo střední společnost viz Obrázek 1, který bude sloužit jako testovací příklad. Vnitřní síť připojená do důvěryhodného rozhraní, servery se nacházejí v DMZ zóně a za nedůvěryhodné považujeme připojení do Internetu. V tomto případě firewall je výchozí bránou pro vnitřní a DMZ síť.

9.1.1. Vnitřní síť (LAN)

Na zvolených firewallech společnosti Juniper, Cisco a Checkpoint se nachází více rozhraní pro lokální síť. Naše testovací topologie má jenom jednu síť, která bude připojena pomocí přepínače do jednoho rozhraní. Protože se jedná o důvěryhodnou zónu, použijeme pro přidělení IP adres DHCP server.
V našem případě pro lokální síť použijeme privátní rozsah IP adres 192.168.1.0/24. Výchozí branou bude adresa 192.168.1.1 přidělena na vnitřní rozhraní firewallu. Tento rozsah je z privátního rozsahu a proto musíme použít překlad adres. V této sítí bychom neměli provozovat žádné síťové služby a proto ideální a v mnoha případech používanou volbou je použití PATu, neboli skrytého překladu (hide nat). Tak se budou z vnějšího pohledu všichni klienti lokální sítě jevit, jako jedná IP adresa, což bude adresa internetového rozhraní firewallu. Toto řešení přináší jistou míru zabezpečení pro vnitřní síť.

9.1.2. DMZ

Chceme-li provozovat síťové služby dostupné z Internetu, měli bychom z důvodu bezpečnosti vždy použít demilitarizovanou zónu pro umístění serverů. V naší síti pro tento účel postačí použít pouze jedno síťové rozhraní. Použijeme veřejný rozsah IP adres, který nám poskytne náš ISP. Doporučuji zvolit statické přiřazení IP adresy. Pro testovací účely jsme zvolili síť 131.207.25.0/28. Výchozí bránou a zároveň adresou DMZ rozhraní na firewallu bude adresa 131.207.25.1/28.

9.1.3. Vnější síť (WAN)

WAN, neboli taky vnější rozhraní je kritickým bodem z pohledu bezpečnosti. Všechen provoz do a z Internetu vede právě tímto rozhraním. Případné útoky z vnější budou vždy vedeny na tento, nebo skrze tento bod. Připojení do Internetu nám poskytuje ISP, který nám přiděli IP adresy. Použil jsem pro naši testovací síť rozsah 131.207.15.0/24. Adresa 131.207.15.100 bude staticky nastavena na firewallu. Tento rozsah je veřejný, tzn. dosažitelný z celého Internetu. V našem laboratorním prostředí internetové připojení nebudeme používat. ISP směrovač zastoupíme naším směrovačem, který bude obsahovat statickou routu do DMZ sítě. Druhé rozhraní směrovače bude v síti 201.8.5.0/24, ve které se bude nacházet vzdálený administrátor. IP správce je 201.8.5.200, a tento počítač budeme rovněž používat k útokům na naši síť.

9.2. Bezpečnostní pravidla pro vnitřní a vnější síť

V této částí se budeme zabývat jak optimálně navrhnout bezpečnostní pravidla. Je to velmi důležité, protože se určuje, kdo bude mít přístup k síťovým zdrojům a jaké omezení budou stanovená mezi jednotlivými sítěmi.

9.2.1. Směr z LAN do WAN a DMZ

Bezpečnostní pravidla pro vnitřní síť si určuje každá společnost svými interními pravidly. Jestliže mají mít stanice v lokální síti možnost připojení do Internetu, tak preferuji použít pravidlo všechno povolit, a potom jednotlivá spojení zakazovat. Naopak je-li spojení do Internetu zakázáno, povolil bych jenom spojení na interní servery v DMZ zóně a výchozím pravidlem by bylo blokovat ostatní spojení.
V testovací síti jsem použil pravidlo povolit všechna spojení. Zaznamenávat provoz pouze podle potřeby, osobně nedoporučuji povolit log v globálních pravidlech, je to zbytečné mrhání systémovými prostředky firewallu, které jsou omezené. Možnost jak nezaplňovat paměť logy je použít externí log server.

9.2.2. Směr z DMZ do LAN a WAN

Spojení z DMZ zóny by měly být omezené na minimum. DMZ zóna už ve své podstatě zakazuje jakýkoli provoz do vnitřní sítě, přičemž provoz do internetu může být povolen, výchozí nastavení jsou různá podle použitého firewallu. Rozhodně bych doporučil zaznamenávat zakázaný provoz do DMZ zóny.

9.2.3. Směr z WAN do DMZ a WAN

V tomto případě platí zřejmé pravidlo, zakázat všechno a povolit provoz pouze na síťové služby v DMZ zóně, které mají být dosažitelné z internetu. Logy zapínat podle lokální politiky, ale minimálně logovat pravidlo, která zakazuje všechen provoz z WAN.

9.2.4. Spojení na samotný firewall

Protože je firewall výchozí branou a při jednom je dosažitelný z internetu, budeme v povolování spojení přímo na bezpečnostní prvek velice obezřetní. Veškerý provoz z vnější sítě bude zakázán, dokonce i ICMP pakety. Výjimkou bude jenom otevřené spojení pro vzdáleného správce. Tady bych se rád zmínil o použití šifrovaných protokolů pro správu. Jestli firewall poskytuje tuto možnost, tak určitě dáme přednost šifrovanému HTTPS oproti HTTP při použití grafického rozhraní (GUI) a službě SSH oproti TELNETu při použití příkazové řádky (CLI). Důvod je zřejmý, když budeme používat nešifrovaný provoz, může se stát, že útočník bude naslouchat spojení a dozví se privátní informace. Výjimkou může být, když se vzdálený uživatel připojuje pomocí VPN tunelu, což už samo o sobě zaručuje šifrovaný provoz přes Internet.

9.3. Konfigurace firewallu

V této kapitole si ukážeme jak nakonfigurovat bezpečnostní mechanismy na jednotlivá zařízení. Kompletní konfigurační soubory najdete v příloze.

Testovací účet na všech firewallech:

Uživatelské jméno: admin
Heslo: password

Pro porovnání použijeme barevné rozlišení pro jednotlivé produkty:

Cisco ASA 5505
Juniper SSG 5
Checkpoint UTM-1 Edge

Nastavení jednotlivých síťových rozhraní:

Vnitřní rozhraní

interface Vlan1
nameif inside //vnitřní síť
security-level 100 //nastavení bezpečnostní úrovně rozhraní
ip address 192.168.1.1 255.255.255.0

set interface "bgroup0" zone "Trust" // vytvoření logické jednotky bgroup0, která vytváří virtuální směrovač pro přiřazené fyzické rozhraní, přiřazení k důvěryhodné zóně
set interface bgroup0 port ethernet0/2 //přiřazení jednotlivých rozhraní do bridge grupy
set interface bgroup0 port ethernet0/3
set interface bgroup0 port ethernet0/4
set interface bgroup0 port ethernet0/5
set interface bgroup0 port ethernet0/6

set interface bgroup0 ip 192.168.1.1/24//nastavení IP adresy na logikcé jednotce
set interface bgroup0 route

set net lan mode enabled hidenat enabled address 192.168.1.1 netmask 255.255.255.0 dhcpserver enabled dhcprange automatic bridge-antispoofing enabled // aktivace IP spoofingu, Dhcp serveru, překladu adres (PAT) na LAN rozhraní, přiřazeni IP adresy

Vnější rozhraní

interface Vlan2
nameif outside
security-level 0
ip address 131.207.15.100 255.255.255.0

set interface "ethernet0/0" zone "Untrust"
set interface ethernet0/0 ip 131.207.15.100/24
set interface ethernet0/0 nat

set net wan mode lan gateway 131.207.15.1 address 131.207.15.100 netmask 255.255.255.0 dns1 131.207.15.1 dns2 131.207.15.1

DMZ rozhraní

interface Vlan5
no forward interface Vlan1 // zákaz komunikace mezi vlan 5 a vlan1
nameif dmz
security-level 50
ip address 131.207.25.1 255.255.255.240

set interface "ethernet0/1" zone "DMZ"
set interface ethernet0/1 ip 131.207.25.1/28
set interface ethernet0/1 route

set net dmz mode disabled hidenat disabled address 131.207.25.1 netmask 255.255.255.240 static dns enabled bridge-antispoofing enabled

Nastavíme překlad adres (PAT)pro celý rozsah interní sítě, které se budou překládat na adresu vnějšího rozhraní:

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0

nastaveno na bezpečnostní politice pro provoz z Trust do Untrust

nastaveno na vnitřním rozhraní: hidenat enabled

Nastavení výchozí cesty do internetu:

route outside 0.0.0.0 0.0.0.0 131.207.15.1 1

set route 0.0.0.0/0 interface ethernet0/0 gateway 131.207.15.1 permanent

nastaveno na vnějším rozhraní: gateway 131.207.15.1

Nastavení SSH a povolení přístupu pro vnitřní síť a pro vzdáleného správce:

aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL

ssh 192.168.1.0 255.255.255.0 inside
ssh 201.8.5.200 255.255.255.255 outside

access-list outside_access_in_1 extended permit tcp host 201.8.5.200 any eq ssh
access-group outside_access_in_1 in interface outside control-plane

set ssh version v2
set ssh enable

set interface ethernet0/0 ip manageable
set interface ethernet0/0 manage ssh
set interface ethernet0/0 manage ssl
set interface ethernet0/0 manage web
set admin manager-ip 201.8.5.200 255.255.255.255

set ssh mode any
Provoz filtrován v bezpečnostní politice

Nastavení základních bezpečnostních pravidel 3/4. vrstvy a aktivovaní na jednotlivých rozhraních:

access-list inside_access_in extended permit ip any any log disable
access-list dmz_access_in extended permit icmp 131.207.25.0 255.255.255.240 any
access-list outside_access_in extended permit tcp any 131.207.25.0 255.255.255.240 object-group DM_INLINE_TCP_2
access-list outside_access_in_1 extended permit tcp host 201.8.5.200 any eq ssh

object-group service DM_INLINE_TCP_2 tcp
port-object eq ftp
port-object eq www

access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
access-group dmz_access_in in interface dmz

set policy id 1 from "Trust" to "Untrust" "Any" "Any" "ANY" nat src permit
set policy id 1

set policy id 2 from "Trust" to "DMZ" "Any" "131.207.25.0/28" "FTP" permit log
set policy id 2
set service "HTTP"
set service "PING"
set log session-init

set policy id 3 from "Untrust" to "DMZ" "Any" "Any" "FTP" permit log
set policy id 3
set service "HTTP"
set log session-init

set policy id 4 from "Untrust" to "DMZ" "Any" "131.207.25.0/28" "ANY" deny log
set policy id 4
set log session-init

set fw level medium
add fw rules service custom action allow src 192.168.1.183 ports 443 protocol tcp index 1 log true

add fw rules service ssh action allow src 192.168.1.183 dest gw ports 22 protocol tcp index 2 log true

add fw rules service custom action allow src any dest 131.207.25.14 ports 80 protocol tcp index 3 log true

add fw rules service custom action allow src any dest 131.207.25.14 ports 21 protocol tcp index 4 log true

add fw rules service ssh action allow src 201.8.5.200 dest gw ports 22 protocol tcp index 5 log true

add fw rules service any action block src any dest gw ports 0 protocol any index 6 log true

Ochrana proti IP-spoofingu.

ip verify reverse-path interface outside

set zone "Untrust" screen ip-spoofing
set zone "Untrust" screen ip-spoofing drop-no-rpf-route

nastaveno na vnitřním (LAN) rozhraní: bridge-antispoofing enabled

Konfigurace obrany proti základním útokům, hluboké inspekce protokolu HTTP a FTP a kontroly na 7. vrstvě:

threat-detection basic-threat
threat-detection scanning-threat

regex _FTP_username "root"

policy-map type inspect ftp FTP_Username_reset
match username regex _FTP_username
reset log

policy-map type inspect http HTTP_URI_filter
parameters
protocol-violation action drop-connection log
match request uri regex _default_gnu-http-tunnel_uri
drop-connection log
match request header non-ascii
drop-connection

policy-map outside-policy
class outside-class
inspect ftp strict FTP_Username_reset
inspect http HTTP_URI_filter
inspect icmp

service-policy outside-policy interface outside

set zone "Untrust" screen icmp-flood
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen icmp-large

set attack group "CS:DMZ DI"
set attack "CS:FTP_USER_DI" ftp-username "cisco" severity medium
*set attack "CS:URL_DI" http-url ".*index.*" severity medium*
set attack group "CS:DMZ DI" add "CS:FTP_USER_DI"
set attack group "CS:DMZ DI" add "CS:URL_DI"

set policy id 3 attack "CS:DMZ DI" action drop ip-action "notify" target "serv" timeout 60

set smartdefense network-security ip-icmp max-ping-size enforce enabled log enabled size 1472
set smartdefense network-security ip-icmp net-quota enforce enabled log enabled max 100
set smartdefense network-security tcp syndefender enforce enabled log enabled log_mode individual timeout 5 ext_only disabled
set smartdefense network-security port-scan host-port-scan num 20 period 10 external-only false log enabled

set smartdefense ai ftp enforce-commands enabled
add smartdefense ai ftp commands command XPWD allowed false
add smartdefense ai ftp commands command SYST allowed false
add smartdefense ai ftp commands command PWD allowed false

9.4. Testovaní bezpečnostních mechanismů

Existují dva základní přístupy k testování firewallů:

- Penetrační testování
- Testování implementace firewallu

Cílem penetračního testování je odhalit bezpečnostní trhliny dané sítě pomocí běžících útoků proti ní. Penetrační testování obsahuje: sběr informací, průzkum sítě a útoky na cíl. Útoky jsou vykonávány nástroji na odhalení zranitelnosti, které ověřují firewall a jeho potenciální bezpečnostní trhliny a jejich využitelnost.

Testování implementace firewallu se zaměřuje na software firewallu, vyšetřují se chyby v implementaci firewallu. Testování implementace firewallu kontroluje, zda software firewallu provádí akce, které má firewall podle nastavených pravidel vykonat, např. pokud pravidlo firewallu má blokovat přijatý paket, ale firewall tento paket přepošle dále, hovoříme o chybě implementace firewallu. Testování implementace firewallu je primárně vykonáváno výrobci pro zvýšení spolehlivosti jejich produktů.

9.4.1. Penetrační testování

K testování firewallů jsme využili linuxovou distribucí BackTrack[9] ve verzi 4. Tato distribuce slouží primárně k penetračnímu testování sítě, proto obsahuje desítky nástrojů, které pávě k tomuto účelu poslouží.

Jako útočníka budeme považovat počítač s IP 201.8.5.200, který je připojen do vnější sítě. Z tohoto počítače budeme spouštět jednotlivé útoky. Útoky budou mířeny na server v DMZ s IP adresou 131.207.25.14. Použité nástroje:

NMAP – slouží pro mapování sítě a získaní informací o otevřených portech a dostupných službách. Při správném nastavení také zjišťuje použitý operační systém.

HPING2 – tento nástroj nám poslouží k vytvoření paketu s podvrženou zdrojovou adresou (ip spoofing) a k vytvoření SYN povodně.

Použité příkazy jednotlivých nástrojů:

nmap -A -PN -sS -p 1-100 131.207.25.14

Přepínač -A slouží k zapnutí detekce operačního systému, -PN k považování všech hostů jako dostupných, vynechání zkoumání hostů, -sS pro použití TCP SYN paketů. Rozsah skenovaných portů byl stanoven na 1-100.

hping2 -S -p 80 -c 10 -a 192.168.1.25 131.207.25.14

Tento příkaz poslouží pro podvržení IP adresy. Přepínače -S -p80 -c10 znamenají použití TCP SYN paketů na portu 80, počet odeslaných paketů se rovná 10. Jako podvrženou adresu použijeme IP z interní sítě 192.168.1.25.

hping2 -S -p 21 -c 1000 -i u100 131.207.25.14

Takto upravený příkaz využijeme k zahlcení serveru SYN pakety, tzv. SYN-flood. Přepínače -S -p 21 -c 1000 -i u100 znamenají, že na portu 21 (FTP) budeme vysílat 1000 SYN paketů, časový interval mezi dvěma pakety bude 100 mikrosekund.

Na aplikační vrstvě budeme ověřovat FTP a HTTP provoz. Pro FTP budeme analyzovat jednotlivé FTP příkazy a nežádoucí budeme filtrovat. Pro filtrování HTTP provozu použijeme regulární výrazy, které poslouží k analýze URL adresy v hlavičce HTTP paketu.

9.4.2. Výsledky jednotlivých útoků

Pro porovnání výsledků firewallů znovu použijeme barevné rozlišení:

Cisco ASA 5505
Juniper SSG 5
Checkpoint UTM-1 Edge

Kompletní výpisy z logu se nacházejí v příloze.

Skenování portů

Výpis z příkazové řádky po dokončení příkazu nmap.

```
Interesting ports on 131.207.25.14:
Not shown: 98 filtered ports

PORT   STATE SERVICE VERSION
21/tcp open  ftp?
|_ ftp-bounce: no banner
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu))
|_ html-title: Site doesn't have a title (text/html).

Device type: general purpose|remote management|broadband router|phone|VoIP
phone
Running (JUST GUESSING) : Linux 2.6.X (86%), HP embedded (86%), Linksys
embedded (86%), Nokia Symbian OS (86%), Thomson embedded (86%)
Aggressive OS guesses: Linux 2.6.22 (Debian 4.0) (86%), Linux 2.6.24
(Debian) (86%), HP Onboard Administrator management console (86%), HP
Onboard Administrator remote management for BladeSystem server enclosures
(86%), Linksys WRV200 wireless broadband router (86%), Linux 2.6.15
(Ubuntu) (86%), Linux 2.6.15 - 2.6.26 (86%), Linux 2.6.20 (Ubuntu 7.04
server, x86) (86%), Linux 2.6.24 (Ubuntu 8.04) (86%), Linux 2.6.26 (86%)
No exact OS matches for host (test conditions non-ideal).

TRACEROUTE (using port 80/tcp)
HOP RTT  ADDRESS
1   0.36 201.8.5.1
1  1.96 131.207.25.14

Nmap done: 1 IP address (1 host up) scanned in 165.75 seconds

Interesting ports on 131.207.25.14:
Not shown: 98 filtered ports
PORT   STATE SERVICE VERSION

21/tcp open  ftp?
|_ ftp-bounce: no banner
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu))
|_ html-title: Site doesn't have a title (text/html).

Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

TRACEROUTE (using port 80/tcp)
HOP RTT  ADDRESS
1   0.39 201.8.5.1
2    0.79 131.207.15.100
3    1.62 131.207.25.14

Nmap done: 1 IP address (1 host up) scanned in 163.15 seconds

Interesting ports on 131.207.25.14:
Not shown: 98 filtered ports

PORT   STATE SERVICE VERSION
```

```
21/tcp open  ftp?
|_ ftp-bounce: no banner
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu))
|_ html-title: Site doesn't have a title (text/html).

Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26, Linux 2.6.27 (Ubuntu 8.10)

TRACEROUTE (using port 80/tcp)
HOP RTT   ADDRESS
1   0.69  201.8.5.1
2   12.93 131.207.15.100
3   18.66 131.207.25.14
Nmap done: 1 IP address (1 host up) scanned in 166.51 seconds
```

Podvržení IP adresy

Výpisy z logu jednotlivých zařízení:

106021|192.168.1.25||131.207.25.14||Deny TCP reverse path check from 192.168.1.25 to 131.207.25.14 on interface outside

system alert 00008 IP spoofing! From 192.168.1.25:2845 to 131.207.25.14:80, proto TCP (zone Untrust, int ethernet0/0). Occurred 1 times.

Inbound Dropped (by default policy) 192.168.1.25 2886 131.207.25.14 TCP 80 (HTTP) Spoofed IP address -4 WAN

Zahlcení serveru SYN pakety (SYN-flood)

Výpisy z logu jednotlivých zařízení:

302014|201.8.5.200|2568|131.207.25.14|21|Teardown TCP connection 41263 for outside:201.8.5.200/2568 to dmz:131.207.25.14/21 duration 0:00:30 bytes 0 SYN Timeout

system emer 00005 SYN flood! From 201.8.5.200:1884 to 131.207.25.14:21, proto TCP (zone Untrust, int ethernet0/0). Occurred 1 times.

Inbound Reject (by default policy) 201.8.5.200 1227 131.207.25.14 TCP 21 (FTP) SYN Attack

9.4.3. Hluboká inspekce 7. Vrstvy

Pro ověření bezpečnostních mechanismů aplikační vrstvy jsme testovali vytvořením FTP a HTTP provozu, který firewall má zidentifikovat a spojení resetovat, nebo zahodit.

Cisco ASA 5505

Vytvoříme dvě policy mapy pro HTTP a FTP provoz. Typ inspect znamená, že se jedná o hlubokou inspekci 7. vrstvy. V FTP provozu budeme hledat příkaz *username*, který jestli bude roven hodnotě

root, spojení resetujeme. Pro HTTP provoz použijeme výchozí regulární výraz *_default_gnu-http-tunnel_uri*. Pří vyskytnutí se v URL adrese řetězce *index* firewall toto spojení zahodí.

Provoz jsme vytvořili připojením ftp klienta na server s uživatelským jménem *root* 131.207.25.14 a vložením do prohlížeče url adresu *http://131.207.25.14/index.html*.

Výsledkem byly následující hlášení v logu:
FTP provoz:
302014|201.8.5.200|43661|131.207.25.14|21|Teardown TCP connection 41355 for outside:201.8.5.200/43661 to dmz:131.207.25.14/21 duration 0:00:17 bytes 69 Flow closed by inspection
303005|201.8.5.200|43661|131.207.25.14|21|Strict FTP inspection matched username regex _FTP_username in policy-map FTP_Username_reset, Reset connection from outside:201.8.5.200/43661 to dmz:131.207.25.14/21

HTTP provoz:
302014|201.8.5.200|45037|131.207.25.14|80|Teardown TCP connection 41336 for outside:201.8.5.200/45037 to dmz:131.207.25.14/80 duration 0:00:00 bytes 0 Flow closed by inspection
415006|201.8.5.200|45037|131.207.25.14|80|HTTP - matched request uri regex _default_gnu-http-tunnel_uri in policy-map HTTP_URI_filter, URI matched - Dropping connection from outside:201.8.5.200/45037 to dmz:131.207.25.14/80
304001|||||201.8.5.200 Accessed URL 131.207.25.14:/index.html
6|Aug 01 2010|15:59:19|302013|201.8.5.200|45037|131.207.25.14|80|Built inbound TCP connection 41336 for outside:201.8.5.200/45037 (201.8.5.200/45037) to dmz:131.207.25.14/80 (131.207.25.14/80)

Juniper SSG5

Vytvoříme na firewallu skupinu útoku „CS:DMZ DI", do které vložíme jednotlivé útoky:

Hluboká inspekce pro HTTP provoz, resetuje spojení, které obsahuje v HTTP hlavičce URL adresu s výskytem řetězce *index*
útok CS:URL_DI
regulární výraz *".*index.*"*

Hluboká inspekce pro FTP provoz, resetuje spojení, které obsahuje přihlašovací uživatelské jméno *cisco*
útok CS:FTP_USER_DI
příkaz username = cisco

Provoz jsme vytvořili připojením ftp klienta na server s uživatelským jménem *cisco* 131.207.25.14 a vložením do prohlížeče url adresu *http://131.207.25.14/index.html*.

Výsledkem byly následující hlášení v logu:

system warn 00601 CS:URL_DI has been detected from 201.8.5.200/45938 to 131.207.25.14/80 through policy 3 1 times

system warn 00601 CS:FTP_USER_DI has been detected from 201.8.5.200/40880 to 131.207.25.14/21 through policy 3 1 times.

Vytvořili jsme i objekt attack „CS:ftp-dir“ pro filtraci FTP příkazů, který měl filtrovat příkazy pro prohlížení aktuálního pracovního adresáře (PWD, XPWD). Tyto příkazy firewall nebyl schopný identifikovat a spojení pokračovalo s vypsáním adresáře. Použili jsme regulární výraz podle dokumentace, ale bohužel, pokusy se nezdařily. Výrobce neuvádí podporované FTP příkazy.
V firewall logu událostí se nezobrazila, žádná správa.

Přidal jsem do toho objektu ještě příkaz SYST. Jedná se o výpis informaci o FTP serveru. FTP klient po úspěšném přihlášení uživatele automatický odesílá tento příkaz. Tento příkaz firewall rozpoznal a v logu se zobrazila správa o rozpoznání objektu:

warning CS:ftp-dir has been detected from 131.207.15.1/55559 to 131.207.25.14/21 through policy 3 1 times

Checkpoint UTM-1 Edge W

Nastavíme prověřování FTP provozu a zakážeme používat jednotlivé příkazy: PWD, XPWD, SYST. Jedná se o výpis pracovního adresáře a výpis typu operačního systému FTP serveru. Výpis z příkazové řádky ftp klienta:

```
ftp 131.207.25.14

230 User cisco logged in.
ftp> pwd
500 '***': command not understood.
PWD command not recognized, trying XPWD
500 '****': command not understood.
ftp> system
500 '****': command not understood.
ftp> syst
500 '****': command not understood.
ftp>
```

Výpis logu:

Inbound Monitor 201.8.5.200 49075 131.207.25.14 TCP 21 (FTP) FTP illegal command – PWD WAN
Outbound Monitor 131.207.25.14 20 201.8.5.200 TCP 46165 FTP data DMZ
Inbound Monitor 201.8.5.200 49075 131.207.25.14 TCP 21 (FTP) FTP illegal command - PWD WAN

Inbound Monitor 201.8.5.200 49075 131.207.25.14 TCP 21 (FTP) FTP illegal command – SYST WAN

10. Závěr

Na závěr si v jednotlivých krocích shrneme firewally, které jsme testovali a opisovali. Ohodnotíme jednotlivé produkty.

Cisco ASA 5505

- Dokumentace této společnosti pro všechny produkty je velice rozsáhlá, a komplexní. Stejně jako možnosti vzdělávání a získávání certifikátů.
- Bezpečnostní mechanismy jsou porovnatelné mezi všemi třemi výrobci. Větší rozdíly budou určitě ve vyšších produktových řadách.
- Se základní licencí je omezené použití pro tří vlan. Pro třetí vlan je omezený odchozí provoz pouze do jedné předem zvolené vlany.
- Produkt ASA 5505 vyžaduje mnoho znalostí pro konfiguraci. Ale taky jako jediný v porovnání s ostatními poskytuje nejkomplexnější možnosti konfigurace. Tady musím zdůraznit, že jak rozhraní příkazového řádku, který jako jediný podporuje více konfiguračních úrovní, tak grafické rozhraní ASDM, které je na téměř stejné profesionální úrovni jako CLI. Bez znalostí i pomocí grafického režimu bude problematické toto zařízení správně nakonfigurovat. Pro některé se může jevit nevýhodou nutnost instalace grafického softwaru ASDM.
- Při skenování portů (NMAP) jako jediný firewall zamezil správnému určení operačního systému a při provádění tcp sledování, byl schopen ukrýt vnější rozhraní (IP 131.207.15.100).
- Podvržení adresy detekoval úspěšně.
- Při spuštění SYN povodně, jako jediný nedetekoval SYN útok při prvních 1000 paketů (určitě lze použít vhodnější konfigurace pro zamezení útoku). Při spuštění útoku na delší dobu exspirovala výchozí hodnota pro maximální počet paketů za časový interval. Zajímavou funkci je funkce *shun*(vyhýbat se), která úzce spolupracuje z detekcí standardních útoků a poskytuje možnost vyhýbání se a zamítání provozu iniciovaného útočníkovou zdrojovou IP adresou. Jedinou možností jak uvolnit tuto IP adresu, je použít negaci příkazu shun.
- Detekce útoků na sedmé vrstvě byla úspěšná pro FTP i HTTP provoz.

Juniper NetScreen SSG 5

- Dokumentace taky na velmi vysoké úrovni, možnost vzdělávání a získávání certifikátu.
- Bezpečnostní mechanismy poskytují stejné bezpečnostní možností jako u jiných výrobců.
- Tento firewall při zakoupení základní licence poskytuje nejlepší poměr ceny k získaným možnostem. Z důvodu použití odlišné filosofie konfigurace bezpečnostních zón, poskytuje skutečně velice flexibilní možnosti jak využít každé fyzické rozhraní.
- Konfigurace pomocí CLI není tak přehledná jako u zařízení ASA, ale taky poskytuje stále hodně možností. Jestli se jedná o grafické rozhraní, tak to považují za nejpřehlednější. Hlavně výpisy log záznamů jsou podle mého názoru nejlépe vyřešeny. Máme možnost si vypsat všechny záznamy logu, ale kromě toho způsobu máme možnost si vypisovat logy pro jednotlivá bezpečnostní pravidla. Přímo kliknutím na log ikonku v bázi pravidel.

- Při skenování portů si radil firewall velice dobře, jak bylo vidět na výsledku nedokázalo úspěšně zamezit zjištění OS serveru, a skrýt IP adresu na vnějším rozhraní.
- Podvržení adresy úspěšně detekoval.
- Povodeň SYN paketů úspěšně detekoval, s 49% skutečností. Výpisy se nacházejí v příloze.
- Detekce útoků na aplikační vrstvě nedopadla úplně nejlépe. U HTTP provozu mechanismus úspěšně odhalil nechtěný řetězec v URL adrese, ale pro FTP nebyl schopen, na dané konfiguraci, identifikovat některé FTP příkazy.

Check Point UTM-1 Edge W

- Bohužel toto zařízení neposkytuje výbornou dokumentaci jako u ostatních. Příručky se týkají konfigurace zařízení, ale neposkytují podrobnou dokumentaci k funkčnosti bezpečnostních mechanismů. Největší zdroje informací najdete na fórech ze zkušeností administrátorů. Check Point taky nabízí možnost získávání certifikátů a školení.
- Check Point poskytuje nejnovější technologie ochrany, ale na všechna potřebujete licenci, kterou si musíte zakoupit. Toto zařízení vychází cenově nejhůř (nejdražší), a za minimálně dvojnásobnou cenu jako SSG5 neposkytuje žádné velké výhody.
- Největší výhodou je to, že konfigurace pomocí grafického rozhraní je velice intuitivní a poskytuje mnoho průvodců konfigurací zařízení. Bohužel některé nejde vypnout a přidávání jednotlivých pravidel pomocí průvodce je někdy docela únavné. Grafické zpracovaní internetového portálu je opravdu vydařené, a po prvním přihlášení na mně udělalo největší dojem. CLI se nehodí pro konfiguraci toho zařízení, protože aktivace čtyř funkcí v jednom příkazu se mi zdá jako dost nešikovné řešení. Hlavně při čtení konfigurace jsem byl bez konfigurační dokumentace úplně ztracený.
- Během mapování portů si vedl firewall stejně dobře jako NetScreen SSG5.
- Podvržení IP adresy detekoval úspěšně.
- Při útoku SYN-flood měl tento model nejlepší výsledky. 97% paketů zahozeno firewallem.
- Kontrolu na aplikační úrovni zvládl výborně pro FTP provoz. Bohužel z důvodů omezených možností nastavení jednotlivých parametrů, se mi nepodařilo ověřit HTTP provoz.

Každý z uvedených produktů si určitě najde svoje příznivce. Osobně hodnotím Juniper NetScreen SSG5 jako nejvíc vyvážený produkt.

Tato práce by se dále mohla zabývat VPN mechanismy jednotlivých produktů. Vytvoření a testování tunelů mezi firewally odlišných společnosti.

Použitá literatura a zdroje

[1] David Hucaby. Cisco ASA, PIX, and FWSM Firewall Handbook. Indianapolis: Cisco Press 2008, ISBN 1-58705-457-0.

[2] Cisco Security Appliance Command Line Configuration Software Version 8.2. URL: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/asa82cfg.pdf

[3] Juniper Networks, přehled produktů, URL: http://www.juniper.net/us/en/products-services/security/ssg-series/#products

[4] Concepts & Examples, ScreenOS Reference Guide, Release 6.1.0, Rev. 03 URL: http://www.juniper.net/techpubs/software/screenos/screenos6.1.0/ce_all.pdf

[5] Check Point Products & Services, URL: http://www.checkpoint.com/products/index.html

[6] Check Point Software Blades brochure, URL:https://www.checkpoint.com/products/downloads/brochures/SoftwareBlades.pdf

[7] Check Point UTM-1Edge, Embedded NGX 8.0 CLI Reference Guide, URL: http://downloads.checkpoint.com/dc/download.htm?ID=8593

[8] UTM-1Edge, Embedded NGX Version 8.0 - User Guide, URL: http://downloads.checkpoint.com/dc/download.htm?ID=8595

[9] BackTrack – Penetration Testing Distribution, URL: http://www.backtrack-linux.org/

Přílohy

Kořenový adresář:

Složka Cisco

soubory:

- ASAlicence.txt
- konfigurace.txt
- vysledky_backtrack.txt
- log.txt

Složka Checkpoint

soubory:

- UTM-1licence.txt
- konfigurace.cfg
- vysledky_backtrack.txt
- log.xls

Složka Juniper

soubory:

- SSG5licence.txt
- konfigurace.txt
- vysledky_backtrack.txt
- log.txt